

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-73391

(43) 公開日 平成11年(1999) 3月16日

(51) Int.Cl.<sup>8</sup>  
G 0 6 F 15/00  
13/00  
H 0 4 L 9/32  
H 0 4 N 1/44

識別記号  
3 3 0  
3 5 1  
3 5 7

F I  
C 0 6 F 15/00  
13/00  
H 0 4 N 1/44  
7/173

審査請求 未請求 請求項の数16 F D (全 20 頁) 最終頁に続く

(21) 出願番号 特願平9-247580

(22) 出願日 平成9年(1997) 8月29日

(71) 出願人 000005201

富士写真フイルム株式会社  
神奈川県南足柄市中沼210番地

(72) 発明者 椎森 佳子

埼玉県朝霞市泉水三丁目11番46号 富士写  
真フイルム株式会社内

(72) 発明者 太田 義則

埼玉県朝霞市泉水三丁目11番46号 富士写  
真フイルム株式会社内

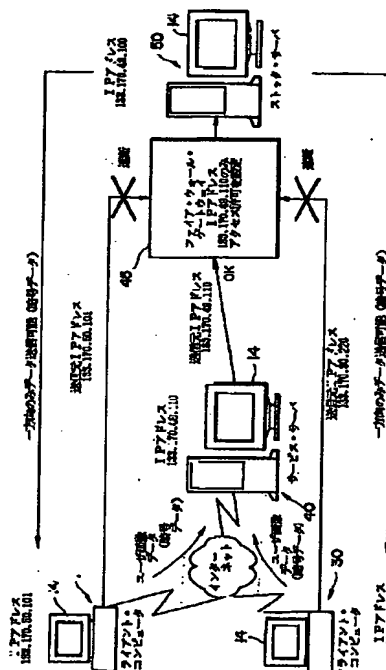
(74) 代理人 弁理士 牛久 健司 (外1名)

(54) 【発明の名称】 データ通信システムおよび方法

(57) 【要約】

【目的】 ストック・サーバ50の破壊を防止する。

【構成】 クライアント・コンピュータ1および30とサービス・サーバ40とがインターネットによって画像データが通信可能に接続されている。ストック・サーバ50はサービス・サーバ40と画像データの通信が可能であるが、クライアント・コンピュータ1および30とはファイア・ウォール45によって画像データの通信が遮断されている。ストック・サーバ50とクライアント・コンピュータ1および30とは、ストック・サーバ50からクライアント・コンピュータ1および30に一方向に画像データの送信が可能である。クライアント・コンピュータ1とストック・サーバ50とは直接にデータ通信できないので、ストック・サーバ50が破壊されないようなデータのみをストック・サーバ50にアップロードできる。



## 【特許請求の範囲】

【請求項1】 複数のクライアント・コンピュータと、サービス・サーバと、ストック・サーバとから構成され、複数の上記クライアント・コンピュータと上記サービス・サーバとは相互にデータ通信可能であり、上記サービス・サーバと上記ストック・サーバとは相互にデータ通信可能であり、複数の上記クライアント・コンピュータと上記ストック・サーバとは上記ストック・サーバから複数の上記クライアント・コンピュータに一方方向にデータ通信が可能である、データ通信システム。

【請求項2】 複数の上記クライアント・コンピュータのうちの1の上記クライアント・コンピュータが、上記サービス・サーバに送信すべきデータを暗号化するクライアント・コンピュータ暗号化手段、および上記クライアント・コンピュータ暗号化手段によって暗号化されたデータを上記サービス・サーバに送信するクライアント暗号データ送信手段を備え、上記サービス・サーバが、上記クライアント・コンピュータ暗号データ送信手段によって送信された暗号化されたデータを復号するサービス・サーバ復号手段、および上記サービス・サーバ復号手段によって復号されたデータを上記ストック・サーバに送信するサービス・サーバ復号データ送信手段を備え、上記ストック・サーバが、上記サービス・サーバ復号データ送信手段から送信されたデータを暗号化するストック・サーバ暗号化手段、上記ストック・サーバ暗号化手段によって暗号化されたデータを、上記サービス・サーバにデータを送信した上記1のクライアント・コンピュータに関連づけて記憶する暗号データ記憶手段、および上記暗号データ記憶手段に記憶されている暗号化されたデータを、関連づけられている上記1のクライアント・コンピュータに送信するストック・サーバ暗号データ送信手段を備え、上記1のクライアント・コンピュータが、上記ストック・サーバ暗号データ送信手段から送信された暗号化されたデータを復号するクライアント・コンピュータ復号手段を備えている、請求項1に記載のデータ通信システム。

【請求項3】 上記1のクライアント・コンピュータが、上記ストック・サーバに記憶されている暗号化されたデータの送信要求を表すデータを上記サービス・サーバに送信する手段を備え、上記サービス・サーバが、上記1のクライアント・コンピュータから送信された送信要求を表すデータを上記ストック・サーバに送信する手段を備え、上記ストック・サーバの上記暗号データ送信手段が、上記サービス・サーバから送信された送信要求を表すデータの受信に応答して、上記暗号データ記憶手段に記憶されている暗号化されたデータを上記1のクライアント・コンピュータに送信するものである、請求項2に記載のデータ通信システム。

【請求項4】 上記1のクライアント・コンピュータが、暗号化されたデータの復号のための鍵を他の上記ク

ライアント・コンピュータに送信する手段をさらに備えている請求項2に記載のデータ通信システム。

【請求項5】 複数の上記クライアント・コンピュータのうちの1の上記クライアント・コンピュータが、上記サービス・サーバにパスワードを送信するパスワード送信手段をさらに備え、上記サービス・サーバが、上記パスワード送信手段から送信されたパスワードが、上記ストック・サーバから送信されるデータを受信する正当なクライアント・コンピュータであることを示す正当なパスワードかどうかを判定するパスワード認証手段、および上記パスワード認証手段により、上記パスワード送信手段から送信されたパスワードが、上記ストック・サーバから送信されるデータを受信する正当なクライアント・コンピュータであることを示す正当なパスワードと判定したことにより、パスワードを送信した1の上記クライアント・コンピュータにデータ送信するように送信指令を送る送信指令送付手段を備えている、請求項1に記載のデータ通信システム。

【請求項6】 上記データは、画像を表す画像データであり、上記サービス・サーバは、上記クライアント・コンピュータから送信された画像データによって表される画像の縮小画像を表す縮小画像データを、画像データを送信した上記クライアント・コンピュータに対応して記憶する手段をさらに備えている、請求項1に記載のデータ通信システム。

【請求項7】 上記ストック・サーバは、画像合成に用いられるテンプレート画像を表すテンプレート画像データを記憶するテンプレート画像データ記憶手段を備え、上記サービス・サーバは、上記テンプレート画像の縮小画像を表す縮小画像データを記憶する手段を備えている、請求項6に記載のデータ通信システム。

【請求項8】 データ通信システムを構成し、かつサービス・サーバとストック・サーバとからなるサーバ・システムであり、上記サービス・サーバは、複数のクライアント・コンピュータと相互に通信可能であり、上記ストック・サーバは上記サービス・サーバと相互に通信可能であり、上記ストック・サーバから複数の上記クライアント・コンピュータに一方方向にデータ通信可能である、データ通信システムを構成するサーバ・システム。

【請求項9】 複数のクライアント・コンピュータと、サービス・サーバと、ストック・サーバとから構成されるデータ通信システムにおいて、複数の上記クライアント・コンピュータと上記サービス・サーバとが相互にデータ通信し、上記サービス・サーバと上記ストック・サーバとが相互にデータ通信し、複数の上記クライアント・コンピュータと上記ストック・サーバとが上記ストック・サーバから複数の上記クライアント・コンピュータに一方方向にデータ通信する、データ通信方法。

【請求項10】 複数の上記クライアント・コンピュータのうちの1の上記クライアント・コンピュータにおい

て、上記サービス・サーバに送信すべきデータを暗号化し、暗号化されたデータを上記サービス・サーバに送信し、上記サービス・サーバにおいて、一の上記クライアント・コンピュータから送信された暗号化されたデータを復号し、復号されたデータを上記ストック・サーバに送信し、上記ストック・サーバにおいて、上記サービス・サーバから送信されたデータを暗号化し、暗号化されたデータを、上記サービス・サーバにデータを送信した上記一のクライアント・コンピュータに関連づけて記憶し、記憶されている暗号化されたデータを、関連づけられている上記一のクライアント・コンピュータに送信し、上記一のクライアント・コンピュータにおいて、上記ストック・サーバから送信された暗号化されたデータを復号する、請求項9に記載のデータ通信方法。

【請求項11】 上記ストック・サーバに記憶されている暗号化されたデータの送信要求を表すデータを、上記一のクライアント・コンピュータから上記サービス・サーバに送信し、上記一のクライアント・コンピュータから送信された送信要求を表すデータを、上記サービス・サーバから上記ストック・サーバに送信する手段を備え、上記サービス・サーバから送信された送信要求を表すデータの受信にตอบสนองして、上記ストック・サーバに記憶されている暗号化されたデータを上記一のクライアント・コンピュータに送信するものである、請求項10に記載のデータ通信方法。

【請求項12】 暗号化されたデータの復号のための鍵を、上記一のクライアント・コンピュータから他の上記クライアント・コンピュータに送信する、請求項10に記載のデータ通信方法。

【請求項13】 複数の上記クライアント・コンピュータのうちの上記クライアント・コンピュータから、上記サービス・サーバにパスワードを送信し、上記サービス・サーバにおいて、一の上記クライアント・コンピュータから送信されたパスワードが、上記ストック・サーバから送信されるデータを受信する正当なクライアント・コンピュータであることを示す正当なパスワードかどうかを判定し、一の上記クライアント・コンピュータから送信されたパスワードが、上記ストック・サーバから送信されるデータを受信する正当なクライアント・コンピュータであることを示す正当なパスワードと判定したことにより、パスワードを送信した一の上記クライアント・コンピュータにデータ送信するように送信指令を送る、請求項9に記載のデータ通信方法。

【請求項14】 上記データは、画像を表す画像データであり、上記サービス・サーバは、上記クライアント・コンピュータから送信された画像データを上記ストック・サーバに送信するとともに、上記クライアント・コンピュータから送信された画像データによって表される画像の縮小画像を表す縮小画像データを、画像データを送信した上記クライアント・コンピュータに対応して記憶

する、請求項9に記載のデータ通信方法。

【請求項15】 上記ストック・サーバには、画像合成に用いられるテンプレート画像を表すテンプレート画像データが記憶されており、上記サービス・サーバには、上記テンプレート画像の縮小画像を表す縮小画像データが記憶されている、請求項14に記載のデータ通信方法。

【請求項16】 データ通信システムを構成し、かつサービス・サーバとストック・サーバとからなるサーバ・システムにおいて、上記サービス・サーバが、複数のクライアント・コンピュータと相互に通信し、上記ストック・サーバが上記サービス・サーバと相互に通信し、上記ストック・サーバから複数の上記クライアント・コンピュータに一方方向にデータ通信する、データ通信システムを構成するサーバ・システムのデータ通信方法。

【発明の詳細な説明】

【0001】

【技術分野】この発明は、複数のクライアント・コンピュータと、サービス・サーバと、ストック・サーバとから構成されるデータ通信システムおよびその通信方法ならびにこのデータ通信システムを構成するサーバ・システムおよびその通信方法に関する。

【0002】

【発明の背景】パーソナル・コンピュータの発展、インターネットなどのネットワークの伸展に伴い、ネットワークを介して、パーソナル・コンピュータとサーバとを接続し、相互にデータ通信することが可能となってきた。パーソナル・コンピュータのユーザは、自分のパーソナル・コンピュータを用いてデータ（画像データ、テキスト・データ（プログラム・データ）など）をサーバにアップロードすることができる。

【0003】データをサーバに自由にアップロードできるとすると、ウイルスを含んだデータのアップロードも可能となり、ウイルスを含んだデータのアップロードによりサーバが破壊されることがある。また、アップロードしたユーザ以外のユーザが自由にアップロードしたデータにアクセスできるとすると、アップロードしたデータが改ざんされることが有り得る。このため、ネットワーク・セキュリティ・システムは非常に重要である。

【0004】従来のネットワーク・セキュリティ・システムには、ファイア・ウォール（fire wall）を利用したシステム、パスワードによる認証システムなどがある。

【0005】ファイア・ウォールを利用したシステムでは、特定のクライアント・コンピュータからのデータのアップロードを認め、特定のクライアント・コンピュータ以外のクライアント・コンピュータからのデータのアップロードを認めないようにしてネットワーク・セキュリティを確保している。しかしながら、ファイア・ウォールを利用したシステムでは、特定のクライアント・コ

ンピュータからしかデータのアップロードが認められないという欠点がある。

【0006】パスワードによる認証システムでは、サーバを破壊する悪意をもったクライアント・コンピュータのユーザのアクセスも許可されるので、ネットワーク・セキュリティの確保が困難である。

【0007】

【発明の開示】この発明は、サーバへのデータのアップロードが可能なクライアント・コンピュータを制限することなく、ネットワーク・セキュリティを確保することを目的とする。

【0008】この発明によるデータ通信システムは、複数のクライアント・コンピュータと、サービス・サーバと、ストック・サーバとから構成され、複数の上記クライアント・コンピュータと上記サービス・サーバとは相互にデータ通信可能であり、上記サービス・サーバと上記ストック・サーバとは相互にデータ通信可能であり、複数の上記クライアント・コンピュータと上記ストック・サーバとは上記ストック・サーバから複数の上記クライアント・コンピュータに一方向にデータ通信が可能であることを特徴とする。

【0009】この発明は、上記データ通信システムに適した方法も提供されている。すなわち、複数のクライアント・コンピュータと、サービス・サーバと、ストック・サーバとから構成されるデータ通信システムにおいて、複数の上記クライアント・コンピュータと上記サービス・サーバとが相互にデータ通信し、上記サービス・サーバと上記ストック・サーバとが相互にデータ通信し、複数の上記クライアント・コンピュータと上記ストック・サーバとが上記ストック・サーバから複数の上記クライアント・コンピュータに一方向にデータ通信するものである。

【0010】この発明によると、複数の上記クライアント・コンピュータと上記サービス・サーバ、上記サービス・サーバと上記ストック・サーバとはそれぞれ相互に通信可能であるが、複数の上記クライアント・コンピュータと上記ストック・サーバとは上記ストック・サーバから複数の上記クライアント・コンピュータに一方向にデータ通信が可能である。複数の上記クライアント・コンピュータから上記ストック・サーバには直接データを送信できない。

【0011】上記クライアント・コンピュータからデータをアップロードするときには、データは上記クライアント・コンピュータから上記サービス・サーバに送信される。上記サービス・サーバに送信されたデータは、上記サービス・サーバから上記ストック・サーバに送信され、記憶される。

【0012】上記クライアント・コンピュータから上記ストック・サーバに直接データを送信できず、上記サービス・サーバにデータを送信し、上記サービス・サーバ

から上記ストック・サーバにデータを送信するので、上記サービス・サーバのオペレータは、上記クライアント・コンピュータから送信されたデータを上記ストック・サーバに送信する前にたとえばウイルスが含まれていないかどうかチェックできる。ウイルスを含んだデータを排除でき、上記ストック・サーバを保護できる。

【0013】アップロードするクライアント・コンピュータを制限することなく、上記ストック・サーバを保護できる。

【0014】上記データ通信システムを構成する上記サービス・サーバおよび上記ストック・サーバを単独で構成することもできる。

【0015】上記において、複数の上記クライアント・コンピュータのうちの上記クライアント・コンピュータにおいて、上記サービス・サーバに送信すべきデータを暗号化し、暗号化されたデータを上記サービス・サーバに送信し、上記サービス・サーバにおいて、一の上記クライアント・コンピュータから送信された暗号化されたデータを復号し、復号されたデータを上記ストック・サーバに送信し、上記ストック・サーバにおいて、上記サービス・サーバから送信されたデータを暗号化し、暗号化されたデータを、上記サービス・サーバにデータを送信した上記一のクライアント・コンピュータに関連づけて記憶し、記憶されている暗号化されたデータを、関連づけられている上記一のクライアント・コンピュータに送信し、上記一のクライアント・コンピュータにおいて、上記ストック・サーバから送信された暗号化されたデータを復号することが好ましい。

【0016】上記クライアント・コンピュータから上記サービス・サーバに送信されるデータおよび上記ストック・サーバに記憶されているクライアント・コンピュータからアップロードされたデータはすべて暗号化されているので、アップロードされたデータにアクセスする正当な権限のないクライアント・コンピュータのユーザがアクセスできたとしてもデータを保護することができる。

【0017】さらに、上記ストック・サーバに記憶されている暗号化されたデータの送信要求を表すデータを上記一のクライアント・コンピュータから、上記サービス・サーバに送信し、上記一のクライアント・コンピュータから送信された送信要求を表すデータを上記サービス・サーバから、上記ストック・サーバに送信する手段を備え、上記サービス・サーバから送信された送信要求を表すデータの受信にตอบสนองして、上記ストック・サーバに記憶されている暗号化されたデータを上記一のクライアント・コンピュータに送信するものであることが好ましい。

【0018】上記ストック・サーバから上記クライアント・コンピュータに送信されるデータも暗号化されているので、上記ストック・サーバから正当なユーザのクラ

クライアント・コンピュータにデータを送信する場合に、正当な権限のないクライアント・コンピュータのユーザがデータをアクセスすることができたとしてもデータを保護することができる。

【0019】データをアップロードした一のクライアント・コンピュータから他のクライアント・コンピュータに、復号のための鍵を送信できるようにしてもよい。この場合は、一のクライアント・コンピュータのユーザが他のクライアント・コンピュータのユーザに正当権限を与えることとなり、正当権限を得た（復号のための鍵を得た）他のクライアント・コンピュータのユーザが上記ストック・サーバから送信された暗号化されたデータを受信し、復号できることとなる。

【0020】好ましくは、複数の上記クライアント・コンピュータのうちの一個の上記クライアント・コンピュータから、上記サービス・サーバにパスワードを送信し、上記サービス・サーバにおいて、一の上記クライアント・コンピュータから送信されたパスワードが、上記ストック・サーバから送信されるデータを受信する正当なクライアント・コンピュータであることを示す正当なパスワードかどうかを判定し、一の上記クライアント・コンピュータから送信されたパスワードが、上記ストック・サーバから送信されるデータを受信する正当なクライアント・コンピュータであることを示す正当なパスワードと判定したことにより、パスワードを送信した一の上記クライアント・コンピュータにデータ送信するように送信指令を送る。

【0021】パスワード認証により、上記ストック・サーバから送信されるデータを受信できる正当なクライアント・コンピュータであることが認識でき、正当なクライアント・コンピュータが上記ストック・サーバから送信されるデータを受信できる。

【0022】データとして画像データを上記ストック・サーバにアップロードさせるときにはクライアント・コンピュータから送信された画像データによって表される画像の縮小画像を表す縮小画像データを上記サービス・サーバにおいて記憶しても良い。縮小画像についてはすべてのクライアント・コンピュータのユーザがアクセス可能となる。

【0023】画像合成に用いられるテンプレート画像を表すテンプレート画像データを上記ストック・サーバに記憶し、このテンプレート画像の縮小画像であるテンプレート縮小画像データを上記サービス・サーバに記憶することもできる。

【0024】クライアント・コンピュータのユーザは、上記サービス・サーバとアクセスし、上記サービス・サーバに記憶されている画像データと上記テンプレート縮小画像データとをダウンロードし、得られた画像データとテンプレート画像データとから画像の編集を行なう。高画質の編集画像を得る場合には、上記ストック・

サーバに記憶されている画像データの送信要求を上記サービス・サーバに送信し、この送信要求に回答して上記サービス・サーバおよび上記ストック・サーバに記憶されている画像データおよび上記テンプレート画像データを上記ストック・サーバから上記クライアント・コンピュータに送信する。上記クライアント・コンピュータは受信した高画質な画像データおよびテンプレート画像データを用いて高画質な編集画像を生成できる。必要に応じて印刷することとなる。

【0025】

【実施例の説明】

(1) 画像データ通信システム

図1は、この発明の実施例を示すもので画像データ通信システムの全体構成を示している。

【0026】画像データ通信システムは、複数のクライアント・コンピュータ（図1では2台）1および30と、サービス・サーバ40と、ファイア・ウォール・ゲートウェイ45と、ストック・サーバ50とから構成されている。

【0027】複数のクライアント・コンピュータ1および30は、インターネットを介してサービス・サーバ40と接続されている。複数のクライアント・コンピュータ1および30とサービス・サーバ40とは相互にデータ通信が可能である。クライアント・コンピュータ1とクライアント・コンピュータ30ともインターネットを介して相互にデータ通信が可能である。

【0028】ストック・サーバ50にはファイア・ウォール・ゲートウェイ45が設けられている。ファイア・ウォール・ゲートウェイ45は特定のIPアドレスを有するクライアント・コンピュータまたはサービス・サーバから送信されたデータをストック・サーバ50に与え、特定のIPアドレス以外のクライアント・コンピュータまたはサービス・サーバから送信されたデータをストック・サーバ50に与えることを遮断するものである。この実施例では、サービス・サーバ40から送信されたデータがファイア・ウォール・ゲートウェイ45を通過してストック・サーバ50に与えられる。ファイア・ウォール・ゲートウェイ45は実際にはソフトウェアによって構成され、ネットワークを管理するサーバによってファイア・ウォール・ゲートウェイ45のソフトウェアが動作し、データの送受信が制限される。

【0029】クライアント・コンピュータ1のIPアドレスは133.170.50.101であり、クライアント・コンピュータ30のIPアドレスは133.170.90.220であり、サービス・サーバ40のIPアドレスは133.170.49.110である。ファイア・ウォール・ゲートウェイ45は133.170.49.110のIPアドレス（サービス・サーバ40のアドレス）を有するクライアント・コンピュータまたはサービス・サーバから送信されるデータをストック・サーバ50に与え、133.170.49.110のIPアドレス以外のIPア

ドレスを有するクライアント・コンピュータまたはサービス・サーバからの送信データを遮断する。

【0030】この実施例においては、サービス・サーバ40とストック・サーバ50とは、相互にデータ通信可能であるが、ストック・サーバ50と複数のクライアント・コンピュータ1および30とは、ストック・サーバ50から複数のクライアント・コンピュータ1または30に一方方向にデータ通信が可能とされている。クライアント・コンピュータ1または30からストック・サーバ50にデータを送信することはできない。

【0031】クライアント・コンピュータ1および30とサービス・サーバ40との間における画像データの送信、ストック・サーバ50とクライアント・コンピュータ1および30との間における画像データの送信は後述のように公開鍵方式による暗号が利用される。もちろん秘密鍵方式を利用してよい。

【0032】図2は、クライアント・コンピュータ1の電気的構成を示すブロック図である。

【0033】クライアント・コンピュータ1の全体の動作はCPU2によって統括される。このCPU2によって後述の暗号化および復号が行なわれる。

【0034】クライアント・コンピュータ1には、ROM3、データを一時記憶するためのRAM4、表示装置14に画像を表示させるためのVRAM12、ROM3からのデータの読出しならびにRAM4およびVRAM12へのデータの書込みおよび読出しを制御するためのメモリ・コントローラ15が含まれている。VRAM12から読出された画像データがDAコンバータ13に与えられることにより、アナログ映像信号に変換され表示装置14に表示される。

【0035】また、クライアント・コンピュータ1にはバス・コントローラ5、メモリ・コントローラ15およびタイマ16が接続されている。

【0036】さらに、クライアント・コンピュータ1には、システムI/Oコントローラ6が接続されている。このシステムI/Oコントローラ6にはクライアント・コンピュータ1のユーザからの操作指令を受け付けるためのキーボード7およびマウス8ならびに画像データを読み取るためのCD-ROMドライブ9およびFDドライブ10ならびにネットワークと接続するためのモデム11が接続されている。

【0037】クライアント・コンピュータ1には外部I/Oコントローラ18が接続されている。この外部I/Oコントローラ18には、フラットベッド・スキャナ21、フィルム・スキャナ22、デジタル・スチル・カメラ23およびHDドライブ24が接続されている。HDドライブ24によってデータの読書きが自在なHD（ハード・ディスク：図示略）に動作プログラムが記憶されている（この動作プログラムは、プログラムを記憶したCD-ROMを後述のCD-ROMドライブ9に装

填し、読取られることによりクライアント・コンピュータ1にインストールされHDに記憶される）。HDに記憶されている動作プログラムを読出すことによりクライアント・コンピュータによって後述の所定の処理が行なわれる。

【0038】さらにハードディスクには、ユーザ画像データの暗号化および復号に用いられる一のクライアント公開鍵、一のクライアント秘密鍵およびユーザ画像データが記憶されている（もっとも秘密鍵は、他人によるハードディスクからの読取りを防ぐためにフロッピー・ディスク等の可搬型記憶媒体に記憶してもよい）。一のクライアント公開鍵および一のクライアント秘密鍵は具体的には1および0の組合せからなるデータ列である。公開鍵方式では、秘密鍵を用いて平文データ（ここでは画像データ）を暗号化し、暗号化されたデータを、その秘密鍵に対応する公開鍵を用いて復号できる。また公開鍵を用いて平文データを暗号化し、暗号化されたデータを、その公開鍵に対応する秘密鍵を用いて復号できる。

【0039】さらにクライアント・コンピュータ1には画像を印刷するためのプリンタ20およびこのプリンタ20を制御するためのプリンタ制御回路19が接続されている。

【0040】ユーザはこのクライアント・コンピュータ1を用いて所望の画像データをストック・サーバ50にアップロードすることとなる。

【0041】サービス・サーバ40およびストック・サーバ50の構成もクライアント・コンピュータ1の構成と同様である。

【0042】（2）ユーザ画像データのアップロード  
図3は、クライアント・コンピュータ1のユーザが自分のもつユーザ画像データをストック・サーバ50にアップロードする処理を示すもので、図4は、図3の処理をフローチャートで示している。

【0043】クライアント・コンピュータ1には上述のように画像データの暗号化のために一のクライアント公開鍵および一のクライアント秘密鍵が記憶されている。

【0044】クライアント・コンピュータ1からの画像データの送信に先立ち、クライアント・コンピュータ1に記憶されている一のクライアント公開鍵がサービス・サーバ40に送信される（ステップ61）。サービス・サーバ40はクライアント・コンピュータ1から送信された一のクライアント公開鍵を受信し、クライアント・コンピュータ1に対応して、記憶する（ステップ71）。クライアント公開鍵がサービス・サーバ40に記憶されると、サービス・サーバ40からクライアント・コンピュータ1に画像データのアップロード指示を表すデータが送信される（ステップ72）。

【0045】サービス・サーバ40から画像データのアップロード指示を表すデータが送信されると、ストック・サーバ50に記憶させるべきユーザ画像データが一の

クライアント秘密鍵を用いて暗号化される(ステップ62)。暗号化されたユーザ画像データが暗号化された状態でクライアント・コンピュータ1からサービス・サーバ40に送信される(ステップ63)。

【0046】クライアント・コンピュータ1から送信された、暗号化されたユーザ画像データがサービス・サーバ40において受信される。受信した、暗号化されたユーザ画像データは、サービス・サーバ40に記憶されている一のクライアント公開鍵を用いて復号される(ステップ93)。復号によって得られたユーザ画像データによって表されるユーザ画像がサービス・サーバ40に接続されている表示装置14に表示される(ステップ74)。

【0047】表示装置14に表示されたユーザ画像をサービス・サーバ40のオペレータが実際に目で見てそのユーザ画像を表すユーザ画像データをストック・サーバ40に記憶させてもよいかどうかを判断する。

【0048】この判断の具体的基準は、図5に示されている。

【0049】図5を参照して、ユーザ画像データにコンピュータ・ウイルスが含まれていないかがまず、判断される(ステップ91)。コンピュータ・ウイルスが含まれていなければ(ステップ91でYES)、そのユーザ画像データが破壊されていないかが判断される(ステップ92)。ユーザ画像データが破壊されていないければ(ステップ92でYES)、ユーザ画像が倫理上問題のない画像かどうか判断される(ステップ93)。

【0050】倫理上問題のない画像であれば(ステップ93でYES)、サービス・サーバ40のオペレータはユーザ画像データをストック・サーバ50にアップロードさせても良いと判断する(ステップ94、ステップ75でYES)。ステップ91からステップ93の判断のうちいずれか一つでもNOがあれば、サービス・サーバ50のオペレータはユーザ画像データをストック・サーバ50にアップロードできないと判断する(ステップ95、ステップ75でNO)。

【0051】図3および図4に戻って、上述のようにサービス・サーバ40のオペレータによってユーザ画像データをストック・サーバ50にアップロードできないと判断されると(ステップ75でNO)、ストック・サーバ40に記憶されているユーザ画像データは消去される(ステップ76)。つづいて、ユーザ画像データをストック・サーバ50に登録できない旨およびその理由(コンピュータ・ウイルスが含まれている、ユーザ画像データが破壊されている、倫理上問題がある)を示すデータがサービス・サーバ40からクライアント・コンピュータ1に送信される(ステップ77)。

【0052】サービス・サーバ40から送信されたユーザ画像データをストック・サーバ50に登録できない旨

およびその理由を示すデータをクライアント・コンピュータ1において受信すると(ステップ64でYES)、ユーザ画像データをストック・サーバ50にアップロードできない旨およびその理由がクライアント・コンピュータ1の表示装置14に表示される(ステップ65)。

【0053】サービス・サーバ40のオペレータによって、ユーザ画像データをストック・サーバ40にアップロードできると判断されると(ステップ75でYES)、サービス・サーバ40において復号されたユーザ画像データがサービス・サーバ40からストック・サーバ50に送信される(ステップ78)。

【0054】復号されたユーザ画像データがストック・サーバ50において受信される。すると、ストック・サーバ50において受信したユーザ画像データがストック・サーバ50に記憶されているサーバ秘密鍵を用いて暗号化される(ステップ85)。このようにして暗号化されたユーザ画像データと、ユーザ画像データの暗号化に用いたサーバ秘密鍵と、暗号化に用いたサーバ秘密鍵に対応するサーバ公開鍵とがデータベース・キーによって管理される(ステップ86)。

【0055】暗号化されたユーザ画像データ、暗号化に用いたサーバ秘密鍵およびサーバ公開鍵を管理するデータベース・キーおよびサーバ公開鍵がストック・サーバ50からサービス・サーバ40に送信される(ステップ87)。

【0056】データベース・キーおよびサーバ公開鍵がサービス・サーバ40において受信されると、受信したデータベース・キーとストック・サーバ名(IPアドレス)とにもとづいてサーバ・パスワードが発行され、この発行されたサーバ・パスワードのもとにデータベース・キーおよびサーバ公開鍵がストック・サーバ名とともに管理される(ステップ79、80)。

【0057】発行されたサーバ・パスワードおよびサーバ公開鍵が、対応するクライアント・コンピュータ1のクライアント公開鍵を用いて暗号化される(ステップ81)。暗号化されたサーバ・パスワードおよびサーバ公開鍵がサービス・サーバ40からクライアント・コンピュータ1に送信される(ステップ82)。

【0058】クライアント・コンピュータ1において、暗号化されたサーバ・パスワードおよびサーバ公開鍵が受信されると、サーバ・パスワードおよびサーバ公開鍵に用いたクライアント公開鍵に対応するクライアント秘密鍵を用いて復号される(ステップ66)。復号されたサーバ・パスワードおよびサーバ公開鍵がクライアント・コンピュータ1に記憶される。このようにして記憶されたサーバ・パスワードおよびサーバ公開鍵は、後述のようにストック・サーバ50に記憶されたユーザ画像データをダウンロードし、暗号化されたユーザ画像データを復号)するときに用いられる。

【0059】ユーザ画像データをストック・サーバ50

にアップロードしているので、クライアント・コンピュータ1から削除できる。ユーザ画像データが必要であれば、ストック・サーバ50からダウンロードすることとなる。

【0060】(3)ユーザ画像データの再アップロード  
図6はストック・サーバ50に画像データをアップロードしたことがあるクライアント・コンピュータ1のユーザが再びストック・サーバ50に画像データをアップロードする場合の再アップロード処理を示しており、図7は図6に示す再アップロード処理の手順を示すフローチャートである。

【0061】上述のように、ストック・サーバ50に画像データを一度記憶したユーザのクライアント・コンピュータ1には一のクライアント公開鍵および一のクライアント秘密鍵のほかにサーバ公開鍵が記憶されている。また、ストック・サーバ50にはクライアント・コンピュータ1に対応してデータベース・キーが記憶されている。

【0062】ストック・サーバ50に再び画像データを記憶させるべきクライアント・コンピュータ1のユーザは、ユーザ画像データのアップロード要求および記憶しているサーバ・パスワードをサービス・サーバ40に送信する(ステップ101)。

【0063】サービス・サーバ40がクライアント・コンピュータ1から送信されるアップロード要求およびサーバ・パスワードを受信すると、受信したサーバ・パスワードが解析され、そのサーバ・パスワードによって管理されているサービス・サーバ40に記憶されている一のクライアント公開鍵が読み取られる(ステップ106)。このサーバ・パスワードの解析において、クライアント・コンピュータ1から送信されたサーバ・パスワードが正当なサーバ・パスワードかどうかも判別される。正当なサーバ・パスワードでなければ、サービス・サーバ40からクライアント・コンピュータ1にストック・サーバ50への画像データのアップロードを拒否する旨およびその理由を示すデータがサービス・サーバ40からクライアント・コンピュータ1に送信される(ステップ108)。

【0064】サービス・サーバ40から送信されるストック・サーバ50への画像データのアップロードの拒否の旨を示すデータおよびその理由を示すデータを、クライアント・コンピュータ1が受信すると、その拒否の旨およびその理由がクライアント・コンピュータ1の表示装置14に表示される(ステップ103)。クライアント・コンピュータ1のユーザは、表示装置14の表示を見ることにより必要であれば再度サービス・サーバ40とアクセスすることとなる。

【0065】クライアント・コンピュータ1からサービス・サーバ40に送信されたサーバ・パスワードが正当なサーバ・パスワードであれば(ステップ107でYE

S)、サービス・サーバ40からクライアント・コンピュータ1にユーザ画像データのアップロード指示を示すデータが送信される(ステップ109)。

【0066】サービス・サーバ40から送信されるアップロード指示を示すデータを、クライアント・コンピュータ1が受信すると、ストック・サーバ50にアップロードすべきユーザ画像データが、一のクライアント秘密鍵を用いて暗号化される(ステップ104)。暗号化されたユーザ画像データがクライアント・コンピュータ1からサービス・サーバ40に送信される(ステップ105)。

【0067】クライアント・コンピュータ1から送信された暗号化されたユーザ画像データを、サービス・サーバ40が受信すると、クライアント・コンピュータ1においてユーザ画像データの暗号化に用いられた一のクライアント秘密鍵に対応する一のクライアント公開鍵を用いて復号される(ステップ110)。ユーザ画像データが復号されると、解析されたサーバ・パスワードにより管理されているストック・サーバ50の名称およびデータベース・キーが読み取られる(ステップ111)。

【0068】データベース・キーおよび復号されたユーザ画像データはサービス・サーバ40からストック・サーバ50に送信される(ステップ112)。

【0069】サービス・サーバ40から送信されたデータベース・キーをストック・サーバ40が受信すると、受信したデータベース・キーによって管理されているサーバ秘密鍵を用いてサービス・サーバ40から送信されたユーザ画像データが暗号化される(ステップ115)。以前にアップロードされている暗号化された画像データに用いたサーバ秘密鍵と同じサーバ秘密鍵を用いてユーザ画像データが暗号化されることとなる。このようにして暗号化された画像データが以前にアップロードされている暗号化された画像データを管理しているデータベース・キーによってクライアント・コンピュータごと一括管理される。

【0070】(4)ユーザ画像データのダウンロード  
図8は、ストック・サーバ50にアップロードした画像データを、画像データをアップロードしたクライアント・コンピュータ1のユーザにダウンロードする処理を示している。図9は、図8の処理を示すフローチャートである。

【0071】まず、クライアント・コンピュータ1からサービス・サーバ40に、画像データのダウンロードの要求を示すデータがダウンロードすべきユーザ画像データを示すファイル名とともに送信される(ステップ121)。ダウンロード要求を示すデータとともに、ユーザ画像データをダウンロードする正当なクライアント・コンピュータ1のユーザであることを示すサーバ・パスワードおよびダウンロード先であるクライアント・コンピュータ1の名称がクライアント・コンピュータ1からサ



ービス・サーバ40に送信される。

【0072】サービス・サーバ40は、クライアント・コンピュータ1から送信されたサーバ・パスワードを受信すると、受信したサーバ・パスワードを確認する(ステップ131)。

【0073】サーバ・パスワードが正当なものでなければ(ステップ132でNO)、ユーザ画像データのダウンロードが拒否され、その旨が拒否理由とともにサービス・サーバ40からクライアント・コンピュータ1に送信される(ステップ133)。ダウンロードの拒否およびその理由をクライアント・コンピュータ1が受信すると(ステップ122でYES)、ダウンロードの拒否およびその理由がクライアント・コンピュータ1の表示装置14に表示される(ステップ123)。

【0074】サービス・サーバ40において確認されたサーバ・パスワードが正当なものであれば(ステップ132でYES)、確認されたサーバ・パスワードによって管理されているストック・サーバ名およびデータベース・キーが読み取られる(ステップ134)。読み取られたストック・サーバ名によって特定されるストック・サーバ50に、ダウンロードするクライアント・コンピュータ1の名称、ダウンロードするユーザ画像データのファイル名およびデータベース・キーがサービス・サーバ40から送信される(ステップ135)。

【0075】サービス・サーバ40から送信されたデータベース・キーによって管理されている暗号化されているユーザ画像データのうち、サービス・サーバ40から送信された画像データのファイル名をもつユーザ画像データが、暗号化された状態でダウンロード要求をしたクライアント・コンピュータ1に送信される(ステップ137)。

【0076】クライアント・コンピュータ1が、暗号化されたユーザ画像データを受信するとクライアント・コンピュータ1に記憶されているサーバ公開鍵を用いて暗号化されたユーザ画像データが復号される(ステップ124)。復号されたユーザ画像データによって表されるユーザ画像がクライアント・コンピュータ1の表示装置14に表示される(ステップ125)。

【0077】以上のようにして、ユーザ画像データをアップロードしたクライアント・コンピュータ1は、そのアップロードしたユーザ画像データをダウンロードすることができる。

【0078】(5)サーバ公開鍵送信処理

図10は、一のクライアント・コンピュータ1から他のクライアント・コンピュータ30にサーバ公開鍵を送信するときの処理を示している。図11は、図10に示す処理手順を示すフローチャートである。

【0079】一のクライアント・コンピュータ1から他のクライアント・コンピュータ30にサーバ公開鍵を送信することにより、一のクライアント・コンピュータ1

がアップロードし、暗号化されているユーザ画像データを他のクライアント・コンピュータ30がダウンロードし、復号することができる。

【0080】一のクライアント・コンピュータ1がアップロードしたユーザ画像データをダウンロードする許可を与える他のクライアント・コンピュータ30にあらかじめクライアント・コンピュータ1のクライアント・パスワードおよびサーバ・パスワードが一のクライアント・コンピュータ1から送信されている。

【0081】他のクライアント・コンピュータ30から一のクライアント・コンピュータ1にサーバ公開鍵の送信要求を示すデータが送信される(ステップ151)。一のクライアント・コンピュータ1において、他のクライアント・コンピュータ30からサーバ公開鍵の送信要求を示すデータを受信すると、他のクライアント・コンピュータ30が一のクライアント・コンピュータ1によってアップロードしたユーザ画像データをダウンロードする正当なクライアント・コンピュータであることを示すクライアント・パスワードの送信要求を示すデータが一のクライアント・コンピュータ1から他のクライアント・コンピュータ30に送信される(ステップ141)。

【0082】クライアント・パスワードの送信要求を受けた他のクライアント・コンピュータ30は、クライアント・パスワードおよび他のクライアント・コンピュータ30に固有の他のクライアント公開鍵が他のクライアント・コンピュータ30から一のクライアント・コンピュータ1に送信される(ステップ152)。

【0083】他のクライアント・コンピュータ30からクライアント・パスワードが送信されると、送信されたクライアント・パスワードが解析される(ステップ142)。送信されたクライアント・パスワードが正当なパスワードでなければ(ステップ143でNO)、サーバ公開鍵の送信をしない旨を示すデータが一のクライアント・コンピュータ1から他のクライアント・コンピュータ30に送信される(ステップ147)。他のクライアント・コンピュータ30からサーバ公開鍵の送信不許可を示すデータを受信すると(ステップ153でYES)、他のクライアント・コンピュータ30の表示装置14にサーバ公開鍵の送信不許可が表示される。他のクライアント・コンピュータ30のユーザは、表示装置14の表示を見て必要であれば再度一のクライアント・コンピュータ1にサーバ公開鍵の要求を示すデータを送信する。

【0084】他のクライアント・コンピュータ30から送信されたクライアント・パスワードが正当なものであれば(ステップ143でYES)、他のクライアント・コンピュータ30から送信された他のクライアント公開鍵が記憶される(ステップ144)。他のクライアント公開鍵が記憶されると、その他のクライアント公開鍵を

用いてサーバ公開鍵が暗号化される(ステップ145)。暗号化されたサーバ公開鍵が、一のクライアント・コンピュータ1から他のクライアント・コンピュータ30に送信される(ステップ146)。

【0085】他のクライアント・コンピュータ30が、暗号化されたサーバ公開鍵を受信すると他のクライアント・コンピュータ30に記憶されている他のクライアント秘密鍵を用いて復号される(ステップ155)。復号されたサーバ公開鍵が他のクライアント・コンピュータ30に記憶される(ステップ156)。

【0086】一のクライアント・コンピュータ1によってアップロードされた画像データを、他のクライアント・コンピュータ30がダウンロードする場合には、一のクライアント・コンピュータ1から送信されたサーバ・パスワードを用いてサービス・サーバ40にアクセスする。サービス・サーバ40は、他のクライアント・コンピュータ30から送信されたサーバ・パスワードを確認し、そのサーバ・パスワードから上述のようにストック・サーバ50の名称、データベース・キーおよびクライアント公開鍵を得、ストック・サーバ50にアップロードされている暗号化されたユーザ画像データが他のクライアント・コンピュータ30にダウンロードされる。他のクライアント・コンピュータ30にサーバ公開鍵が記憶されるので、ダウンロードした暗号化されたユーザ画像データを、サーバ公開鍵を用いて復号できる。

【0087】(6)他の実施例

図12は、他の実施例を示すもので画像データ通信システムの全体構成を示している。

【0088】上述した実施例では、サービス・サーバおよびストック・サーバはそれぞれ1台ずつであるが、図12に示す実施例では複数のサービス・サーバ(ここでは2台)40Aおよび40Bならびに複数のストック・サーバ(ここでは4台)50A、50B、50Cおよび50Dと複数のクライアント・コンピュータから構成されている。

【0089】さらに、ストック・サーバ50A、50B、50Cおよび50Dにはクライアント・コンピュータからアップロードされたユーザ画像データに加えてユーザ画像の背景画像を表すテンプレート画像の画像データが記憶されている。上述したようにユーザ画像データをダウンロードするときにテンプレート画像データもストック・サーバからクライアント・コンピュータにダウンロードできる。ユーザ画像データおよびテンプレート画像データをダウンロードしたクライアント・コンピュータはダウンロードしたユーザ画像データおよびテンプレート画像データを用いてテンプレート画像データによって表されるテンプレート画像にユーザ画像データによって表されるユーザ画像を合成し、高画質の合成画像を得ることができる。

【0090】さらに、サービス・サーバ40Aおよび4

0Bには、クライアント・コンピュータからストック・サーバ50A、50B、50Cおよび50Dにアップロードしたユーザ画像データによって表されるユーザ画像の縮小画像(ユーザ画像よりも解像度が低い画像)を表す画像データおよびストック・サーバ50A、50B、50Cおよび50Dに記憶されているテンプレート画像データによって表されるテンプレート画像の縮小画像を表す画像データが記憶されている。ユーザ画像データは、クライアント・コンピュータからアップロードされたユーザ画像データによって表されるユーザ画像を間引きすることにより得られる。テンプレート画像の縮小画像を表す画像データもユーザ画像データと同様にストック・サーバ50A、50B、50Cまたは50Dに記憶されているテンプレート画像データによって表されるテンプレート画像の間引くことにより得ることができる。

【0091】クライアント・コンピュータはサービス・サーバ40Aおよび40Bとは自由にアクセスできるから、サービス・サーバ40Aまたは40Bに記憶されているユーザ画像の縮小画像を表す画像データおよびテンプレート画像の縮小画像を表す画像データを、サービス・サーバ40Aまたは40Bからダウンロードし、解像度の低いユーザ画像データおよびテンプレート画像データを用いて画像合成を行なう。印刷などにより高解像度の合成画像が必要なときには上述のようにストック・サーバ50A、50B、50Cまたは50Dから高解像度のユーザ画像データおよびテンプレート画像データをダウンロードすることとなろう。

【図面の簡単な説明】

【図1】画像データ通信システムの全体構成を示している。

【図2】クライアント・コンピュータの電氣的構成を示すブロック図である。

【図3】クライアント・コンピュータからストック・サーバにユーザ画像データをアップロードする処理を示している。

【図4】クライアント・コンピュータからストック・サーバにユーザ画像データをアップロードする処理のフローチャートである。

【図5】ユーザ画像の確認の処理手順を示すフローチャートである。

【図6】ユーザ画像データの再アップロード処理を示している。

【図7】ユーザ画像データの再アップロード処理のフローチャートである。

【図8】アップロードしたユーザ画像データのダウンロードの処理手順を示している。

【図9】アップロードしたユーザ画像データのダウンロード処理手順を示すフローチャートである。

【図10】一のクライアント・コンピュータから他のクライアント・コンピュータにサーバ公開鍵を送信する処

理を示している。

【図11】一のクライアント・コンピュータから他のクライアント・コンピュータにサーバ公開鍵を送信する処理を示すフローチャートである。

【図12】他の実施例を示すもので、画像データ通信システムの構成を示している。

# 【符号の説明】

- 1, 30 クライアント・コンピュータ
- 11 モデム
- 40 サービス・サーバ
- 45 ファイア・ウォール
- 50 ストック・サーバ

Fig.1

【図1】

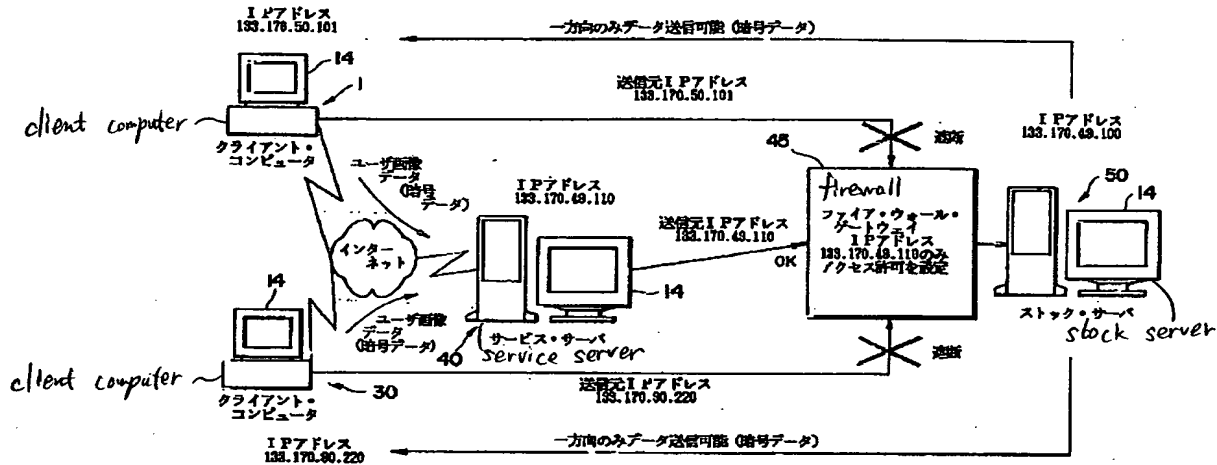


Fig.2

【図2】

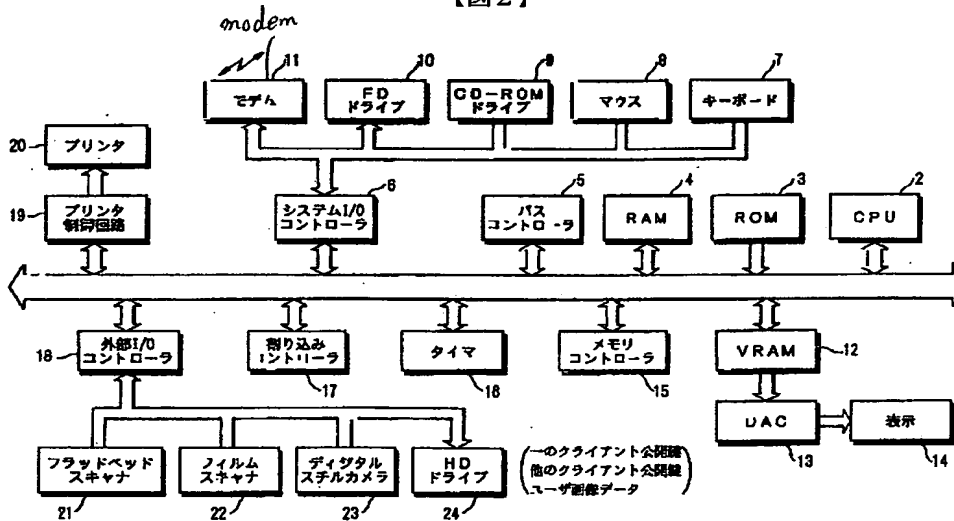
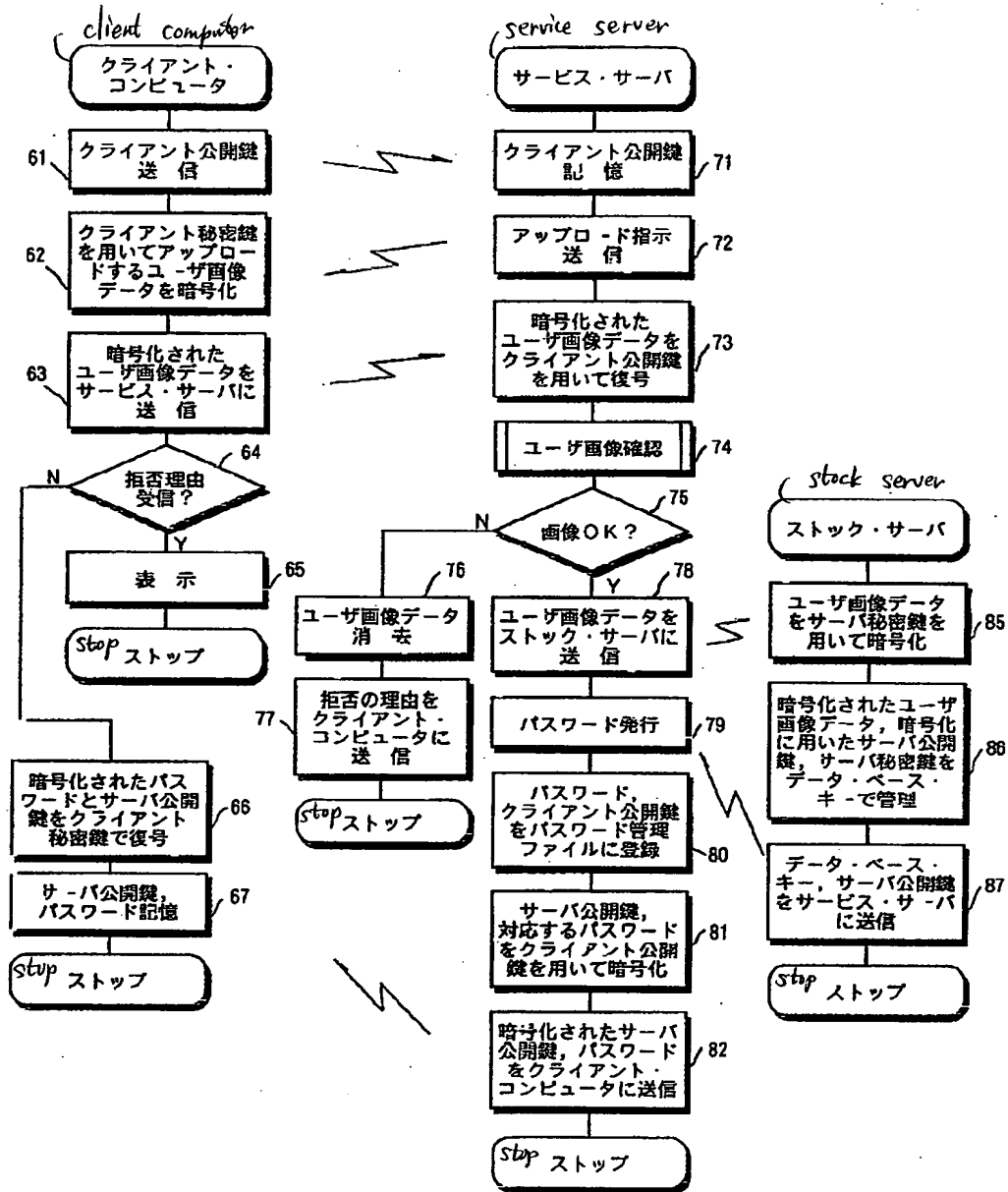
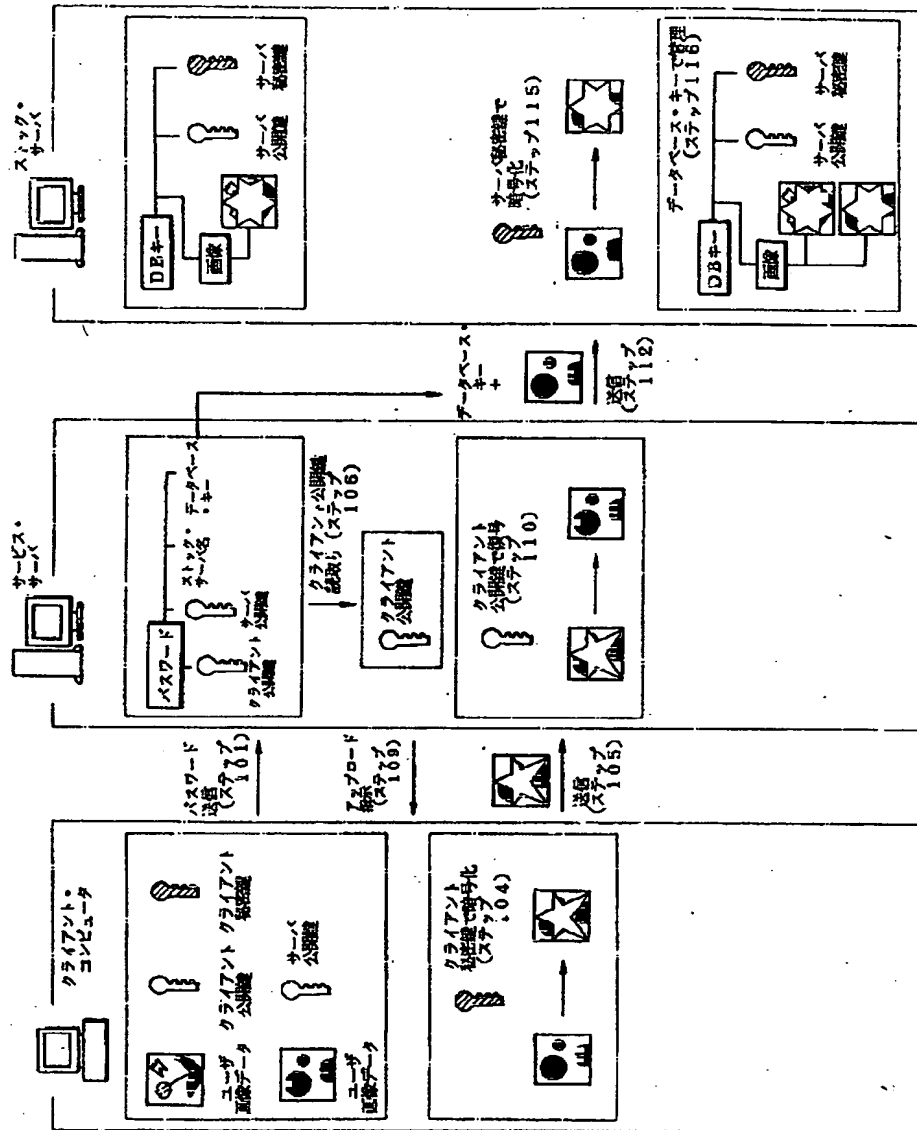




Fig. 4  
 【図4】  
 Image upload process  
 画像アップロード処理

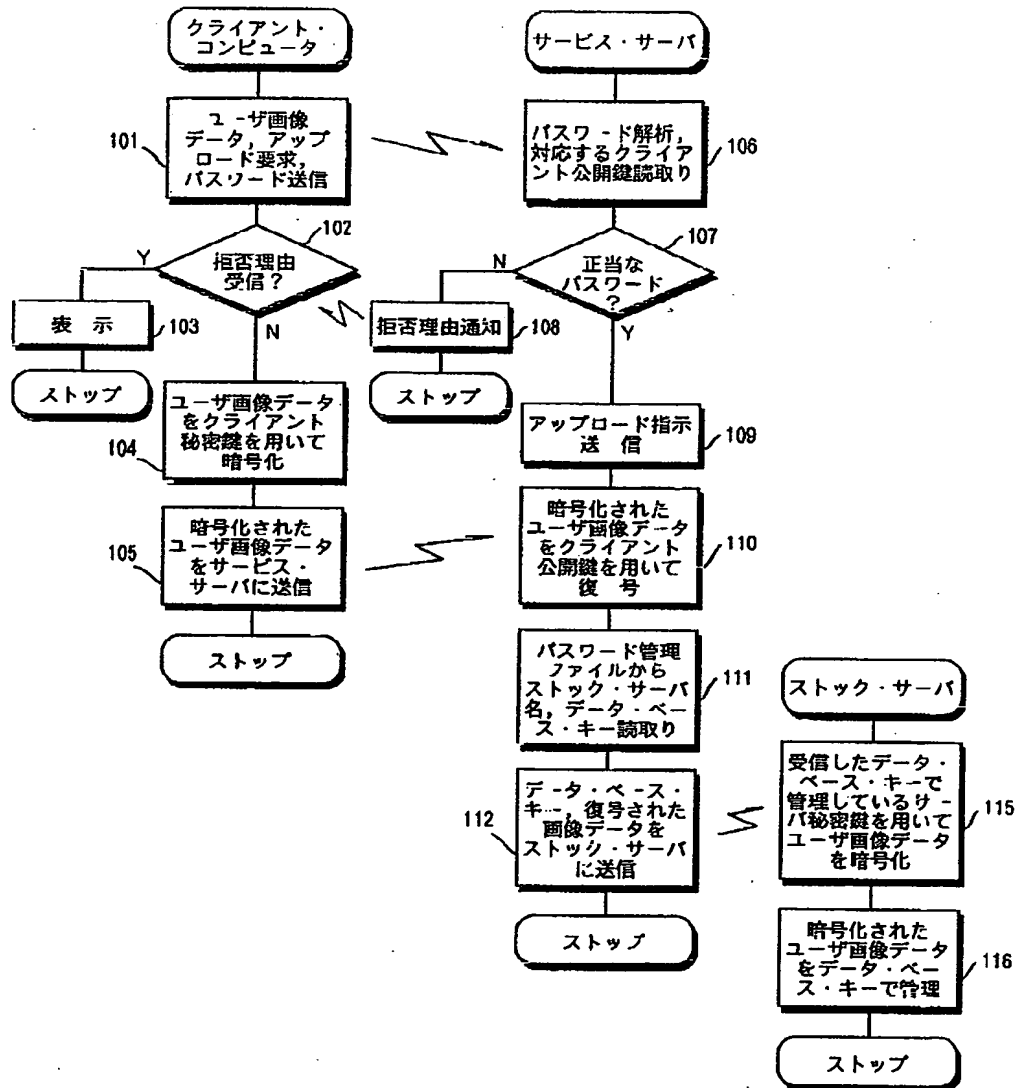


【図6】



【図7】

再アップロード



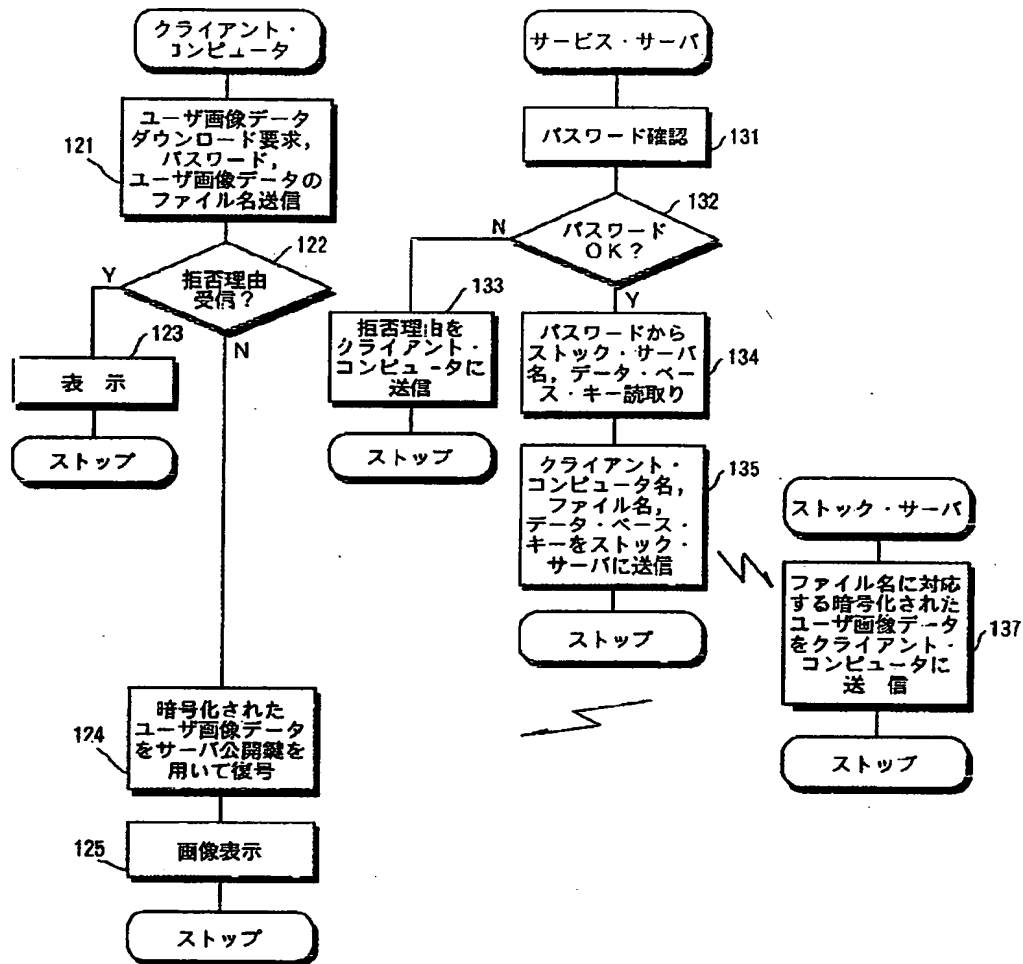
The diagram illustrates the following components and processes:

- System 121 (Left):** Labeled "クライアント・コンピュータ" (Client Computer). It contains a box for "サーバ・パスワード" (Server Password) and a key icon labeled "サーバ公開鍵" (Server Public Key).
- System 131 (Middle):** Labeled "サービス・サーバ" (Service Server). It contains a box for "サーバ・パスワード確認" (Server Password Confirmation), a box for "パスワード" (Password), and a box for "ストリング・データベース" (String Database). It also shows keys for "クライアント公開鍵" (Client Public Key) and "サーバ秘密鍵" (Server Secret Key).
- System 137 (Right):** Labeled "ストック・サーバ" (Stock Server). It contains a box for "DBキー" (DB Key) and a box for "ストリング・データベース" (String Database). It also shows keys for "クライアント公開鍵" (Client Public Key) and "サーバ秘密鍵" (Server Secret Key).
- Data Flow:**
  - An arrow from System 121 to System 131 is labeled "送信要求、パスワード、ファイル名" (Transmission Request, Password, File Name) and "(ステップ 121)".
  - An arrow from System 131 to System 137 is labeled "クライアント・データベース、コンパイル名、データベース・キー" (Client Database, Compile Name, Database Key) and "(ステップ 135)".
  - A return arrow from System 137 to System 131 is labeled "暗号化されたユーザ画像データ" (Encrypted User Image Data) and "(ステップ 137)".

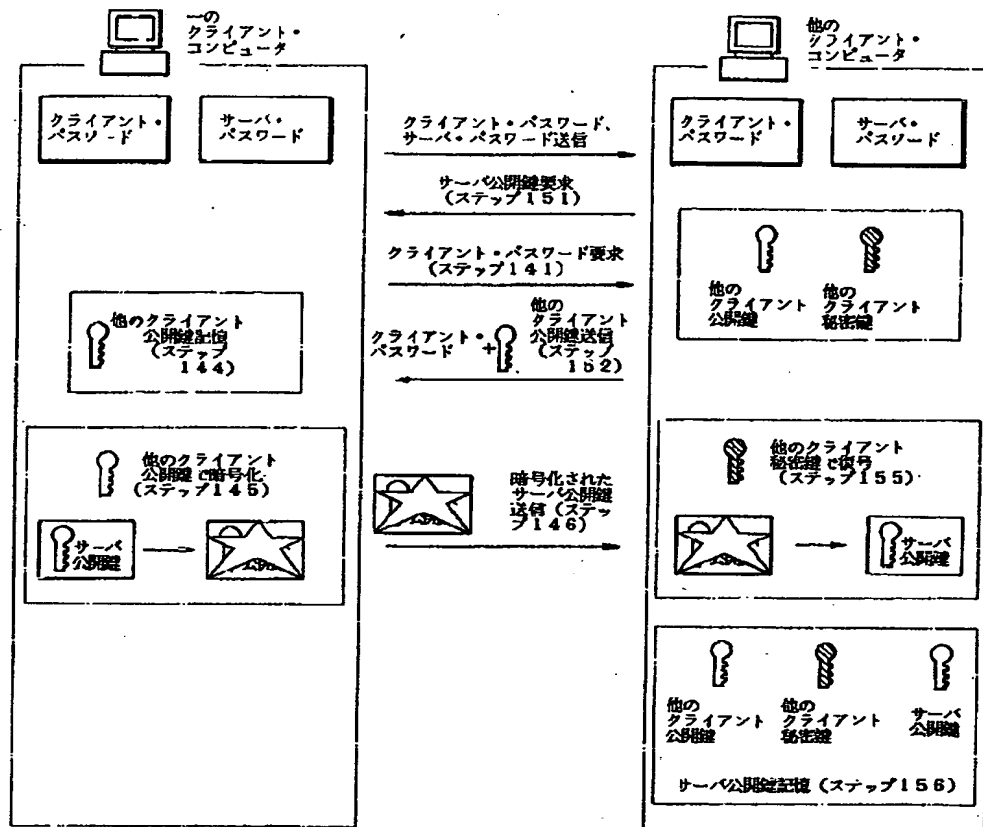


【図9】

## 画像データのダウンロード

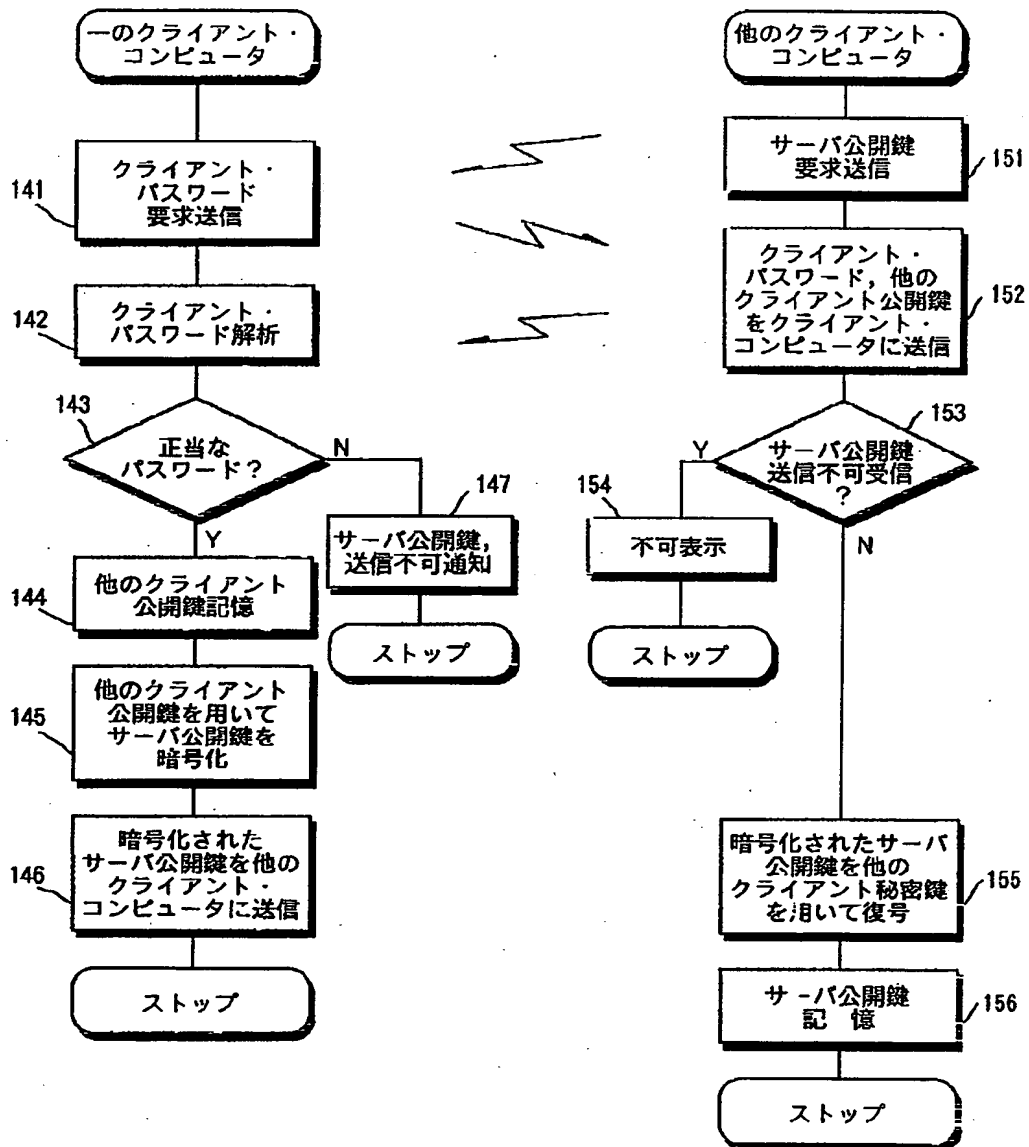


【図10】

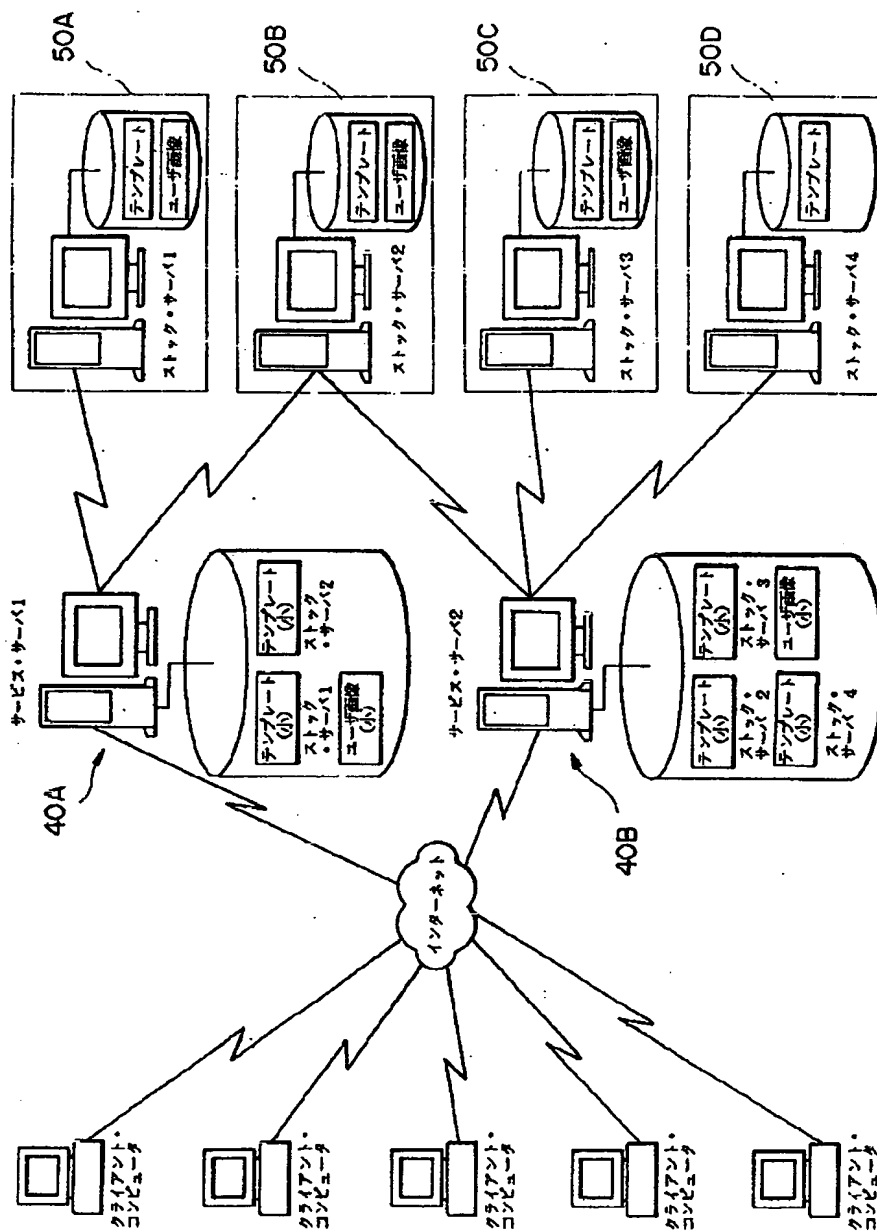


【図11】

## クライアント間のサーバ公開鍵送受信



【図12】



フロントページの続き

(51)Int. Cl.<sup>6</sup>

// H04N 7/173

識別記号

FI

H04L 9/00

673A